

Codec Networks

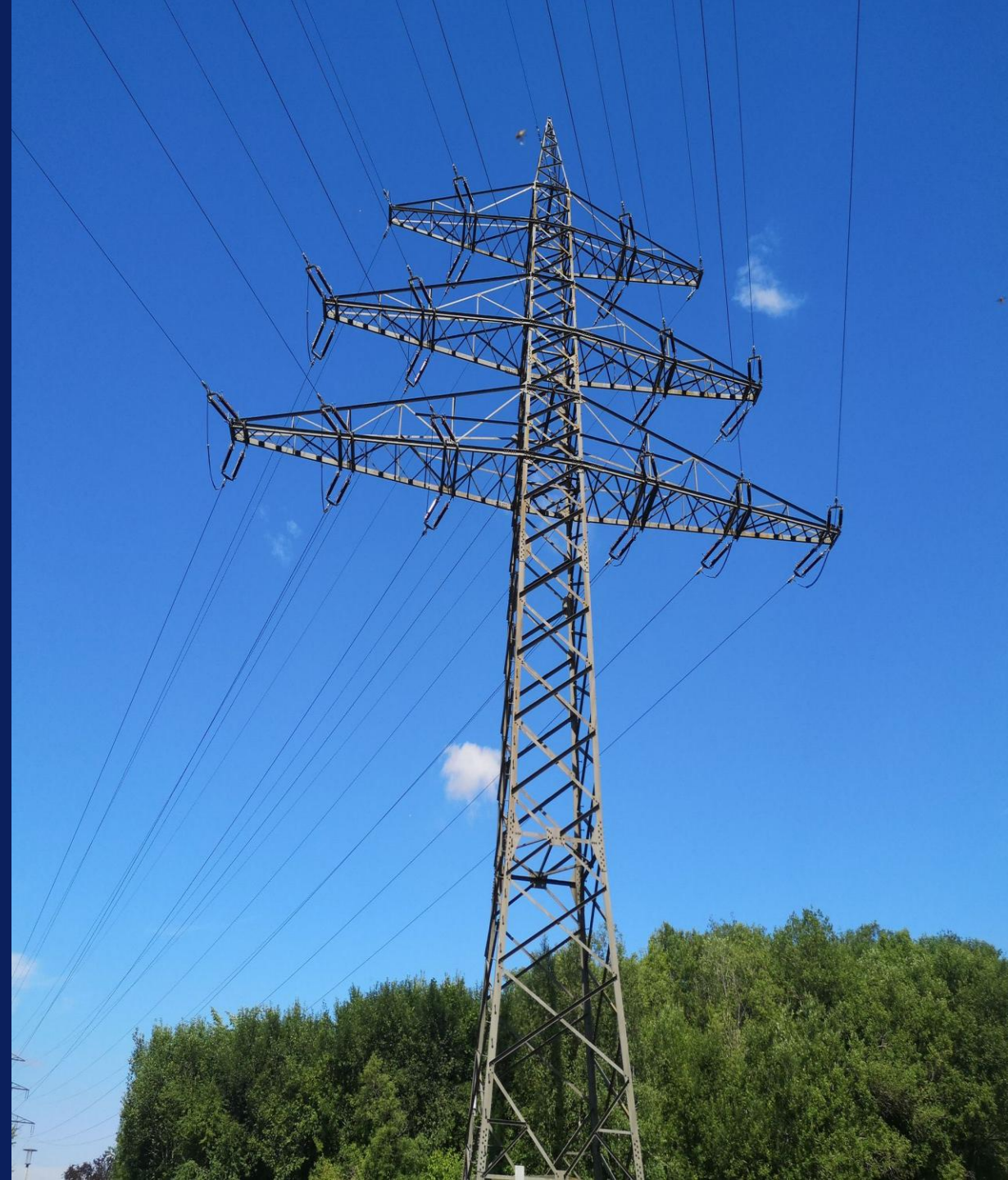
Coding Threats. Decoding Solutions.

POWER & ELECTRICITY

Keep the Lights On. Keep Attackers Out.

IT/OT security, ICS/SCADA assessment, SOC, remote access reviews, resilience and sector compliance for power utilities

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

The CEA Cyber Security Regulations 2026, CERT-In and NCIIPC



How Codec Networks helps

Services, bundles and packages built for the sector



Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



A new rulebook for power sector cybersecurity

The CEA Cyber Security Regulations were notified on 31 July 2026

31 Jul 2026

CEA Cyber Security Regulations notified

1 Apr 2027

Regulations come into force

6 hours

To report incidents to CSIRT-Power and CERT-In (as reported)

50 MW

Threshold for generators and storage under the regulations

What this means: power utilities must appoint a senior CISO, run a 24-hour Information Security Division, maintain a cyber security policy and crisis plan with annual drills, audit critical systems, separate OT from the internet and report incidents quickly (as reported).

Source: CEA (Cyber Security in Power Sector) Regulations, 2026, as reported in public sources.

Who we serve across power and electricity



**Thermal and gas
generators**

Large generating stations



**Hydro and nuclear
operators**

Strategic generation



**Transmission
utilities**

High-voltage networks



**Load dispatch
centres**

Grid operations



DISCOMs

Distribution and metering



**Traders and
exchanges**

Power markets



**Captive and
industrial plants**

Self-generation



**OEMs and
integrators**

Control-system vendors

The threats that cost utilities the most

Six priorities from our 18-threat power sector assessment



Nation-state OT intrusion

Quiet access to grid control



Ransomware into OT

IT incidents reaching plants



Vendor remote access

Permanent tunnels to substations



Smart meter head-ends

Mass disconnect capability



Legacy control systems

Unpatched, flat networks



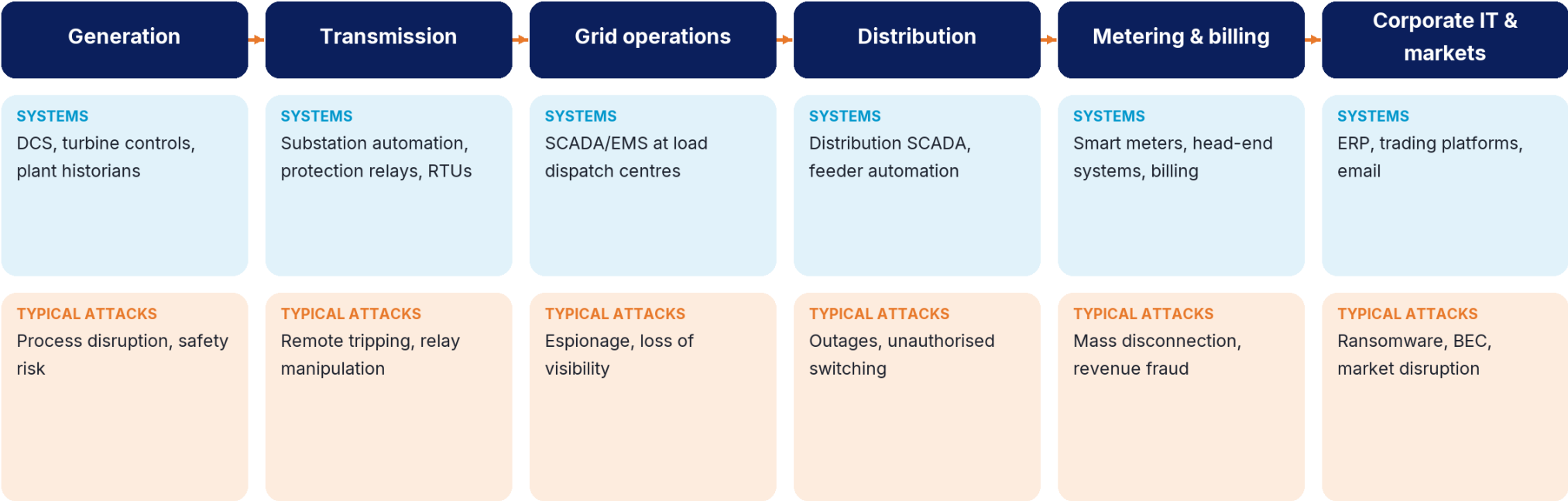
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from plant to meter

Where Cyber Risk Sits Across the Power Value Chain

Every stage from plant to meter carries its own attack surface



Power-sector security must protect operational technology first—IT incidents matter most when they reach the grid.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

The CEA Cyber Security Regulations 2026, CERT-In and NCIIPC

The rules that shape power sector cybersecurity

Requirement	Frequency / deadline	Source
Applicability	OT linked to the grid and connected IT; generators and storage of 50 MW and above	CEA Regulations, 2026
CISO	Senior level, alternate, minimum three-year tenure	CEA Regulations, 2026
Information Security Division	24-hour operation	CEA Regulations, 2026
Cyber Crisis Management Plan	At least one mock drill a year	CEA Regulations, 2026
Audit of critical systems	Annual	CEA Regulations, 2026
Incident reporting	CSIRT-Power and CERT-In within 6 hours	CEA Regulations, 2026; CERT-In
OT network separation	From the internet	CEA Regulations, 2026
Critical information infrastructure	Per notification	NCIIPC (IT Act Section 70)

Key dates on the regulatory timeline

Regulatory Timeline for Power Sector Cybersecurity

Key CEA, Ministry of Power and cross-sector instruments

● In force ● Upcoming (from Oct 2026)

Oct 2021	● CEA Cyber Security Guidelines for the power sector issued
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Aug 2024	● Draft CEA (Cyber Security in Power Sector) Regulations released
Jul 2026	● CEA (Cyber Security in Power Sector) Regulations, 2026 notified (31 July)
Apr 2027	● CEA Cyber Security Regulations come into force (1 April)
May 2027	● Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: CEA, Ministry of Power, CERT-In, MeitY. Confirm obligations against the official gazette notification.

Codec Networks

How Codec Networks helps

IT/OT security · ICS/SCADA · OT SOC · Remote access · Resilience · CEA compliance

One partner from plant to meter



IT/OT Security

Architecture, segmentation, inventory



ICS/SCADA Assessment

SCADA, EMS, DCS, substations



24/7 OT SOC

IT and OT monitoring and hunting



Remote Access Reviews

Vendor access, MFA, recording



Resilience

Crisis plans, drills, recovery



CEA Compliance

Gap assessment, policy, audits

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Captive plants and smaller utilities

- CEA gap assessment (B4)
- IT/OT segmentation review (B3)
- Remote access review (B3)
- Policy pack (B5)

Assurance

State utilities and DISCOMs

- SCADA and substation assessments (B1)
- Smart metering review (B1, B6)
- Annual critical-system audit (B4)
- 24x7 IT/OT SOC (B7)

Continuous Resilience

Large generators, transmission and grid operators

- OT testing and red teaming (B1, B10)
- Threat hunting (B7)
- Crisis plan and drills (B5, B10)
- Board and regulator reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Senior CISO and alternate; 24-hour Information Security Division (CEA Regulations 2026, as reported)	Governance design and CISO support	B5
Cyber security policy and Cyber Crisis Management Plan with annual mock drill (as reported)	Policy, CCMP and drill support	B5, B10
Annual audit of critical systems (as reported)	Independent IT/OT audits	B4, B1
Incidents to CSIRT-Power and CERT-In within six hours (as reported)	OT SOC, IR retainer and reporting support	B7, B8
Separation of OT networks from the internet (as reported)	IT/OT segmentation and remote access review	B3
Vendor accountability and supply-chain security	Vendor and equipment assessments	B9
Consumer and smart meter data safeguards (DPDP)	DPDPA programme for DISCOMs	B6

Five new case studies, five broken chains

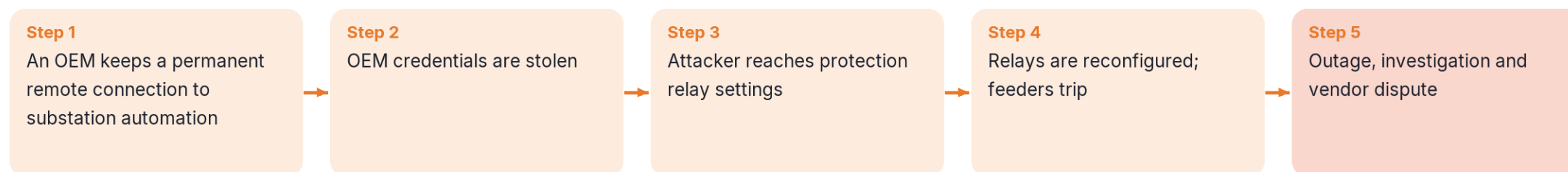
Illustrative composite scenarios written for 2026—not client engagements

1	The Load Dispatch Centre Intrusion	A state-linked group probes for SCADA paths; separation and hunting stop it	B7 · B3 · B8
2	The Substation Remote Access Nobody Logged	Stolen OEM access trips feeders; brokered access prevents it	B3 · B9 · B7
3	The DISCOM Billing Ransomware	Ransomware stops billing and probes SCADA; segmentation contains it	B7 · B10 · B8
4	The Smart Meter Head-End That Could Switch Off a City	Weak head-end controls enable mass disconnects; approvals prevent it	B1 · B2 · B7
5	The Plant DCS on the Corporate Network	Malware disrupts DCS; a plant DMZ prevents it	B3 · B1 · B10

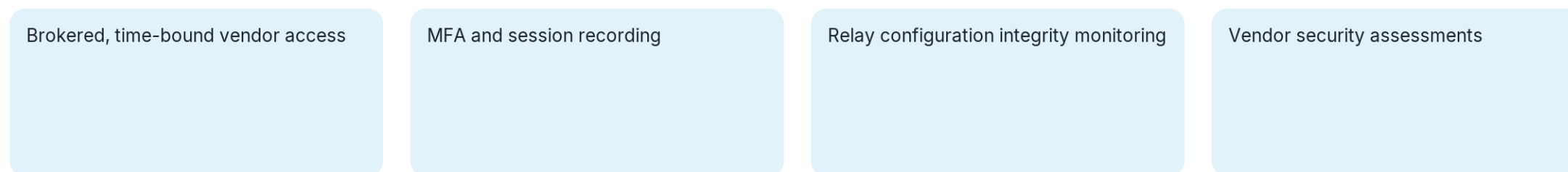
Example: breaking a vendor-access chain

Case 2: The Substation Remote Access Nobody Logged

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: inventory of vendor connections, brokered and time-bound access, MFA and session recording, relay configuration integrity monitoring, and the CSIRT-Power and CERT-In reporting steps.

Why utilities choose Codec Networks



CERT-In empanelled

For information security auditing services; NICSi empanelled for application audits



Certified

ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 20000-1:2018



Regulation-mapped

Mapped to the CEA Regulations 2026, CERT-In, NCIIPC and DPDP



Tests the whole chain

Technical, process and monitoring tests together



Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected



Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Assets, control systems, vendors, metering and compliance calendar

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

 New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

 Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

 011 430 496 96 · 011 437 522 99 · +91 99716 76124 · +91 88007 88220 · +91 88003 31124

 mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities.